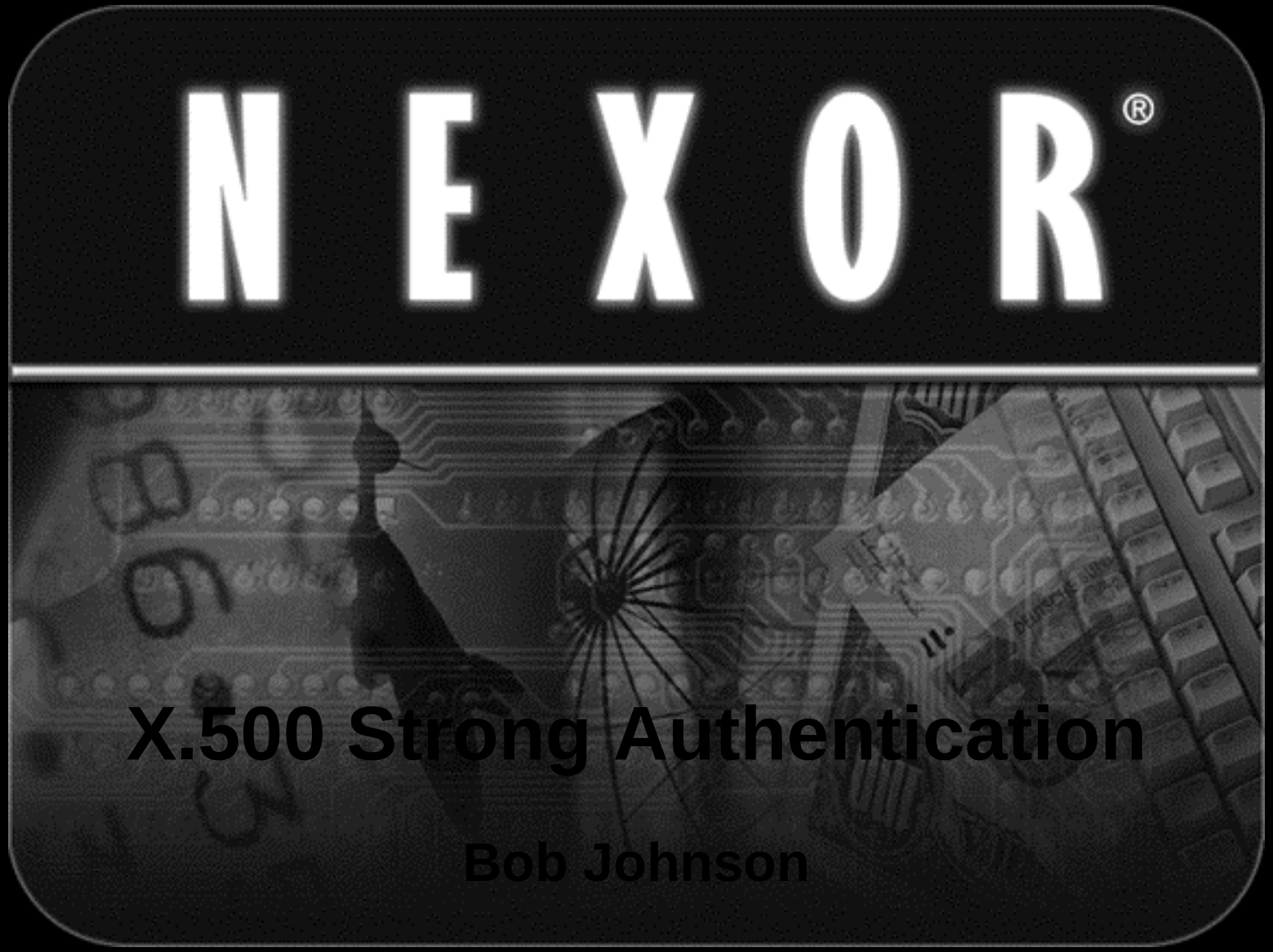


X.500 Strong Authentication

Bob Johnson

NEXOR

Objectives

- What is strong authentication ?
- Who needs strong authentication ?
- Progress report

NEXOR

What is Strong Authentication ?

- **Establishes trust between X.500 directory components, validates identity of directory users for access control, and protects against replay and denial-of-service attacks**
- **Technically speaking…**
  - 2-way digital signature exchange between peer entities w/random number to detect replays (“signed binds”)
  - User’s digital signature on directory requests is verified in order to validate identity of user (“signed operations”)
  - Requests can also be digitally signed by DSAs when chaining the request to a peer DSA (“signed DSP”)
- **As specified in…**
  - X.501, X.509, X.518 ITU Recommendations
  - SDN 705, “Strong Authentication for X.500”

NEXOR

Who needs strong authentication ?

- **If you are using X.500 directory technology and want to…**
  - Protect against unauthorized modification of information stored in your directory
  - Prove the identity of your users and prevent unauthorized access and modification of sensitive information
  - Protect your directory against various forms of attack, including denial-of-service and replays (spoofing)

  …then you need strong authentication.
- **Types of data which require this protection**
  - PKI, PKI, and PKI
  - Other sensitive info - SSN's, home phone #s, pay grades
  - Did we mention PKI?

NEXOR

Why does PKI require strong authentication ?

- **X.509 public key certificates are stored in the directory**
- **X.500 is also used to authenticate certificates**
  - Certificate Revokation Lists
  - Certificate Path Authentication
  - Common “Trust Points” or cross-certification
- **X.509 certificates are an attractive target for**
  - Snooping
  - Removal
  - Substitution
  - Denial of Service
- ***If you can’t trust the keys (certs), retrieve them when needed, prove they’re issued by a trusted certificate authority, and ensure that they haven’t been compromised or revoked…what good is your PKI ???***

NEXOR

Progress Report

- **Supporting working groups**
  - Key Privilege & Certificate Management (KPCM)
  - ACP 133 Task Force
- **Demo'd strong authentication for Harris DMS bid (1993)**
- **Currently updating directory server product**
  - SDN 705
  - FORTEZZA crypto token support
  - ACP 120 and ACP 133 schema
  - PKIX, US Government schema
- **Interoperability testing**
  - Signed binds w/Wang High Assurance Guard, DCL DSA
  - Will test signed ops when avail in other "products under test"
- **Will support non-DMS PKI's (CyberTrust, Xcert, PKIX, etc.)**

NEXOR

Summary

- Strong authentication protects against unauthorized modification of directory information, and is required to enforce access control based on requestor identity
- NEXOR implemented strong authentication in 1993, and is updating their directory products to the latest versions of ACP 133 & SDN 705 with Fortezza cards
- NEXOR is performing interoperability testing with DMS directory & firewall products, as well as several popular commercial PKI offerings
- Strong authentication option for Messageware Directory and Directory Guardian testing now, commercial availability later this year

NEXOR's Business

NEXOR designs, develops and provides enhanced messaging and directory solutions to mission critical environments such as the Military, Intelligence Communities, and Financial Institutions

Gaithersburg, MD

Nottingham, UK

NEXOR®

NEXOR's Pedigree

- NEXOR is focused on Mission Critical Messaging
  - Military, Intelligence, Government and Finance

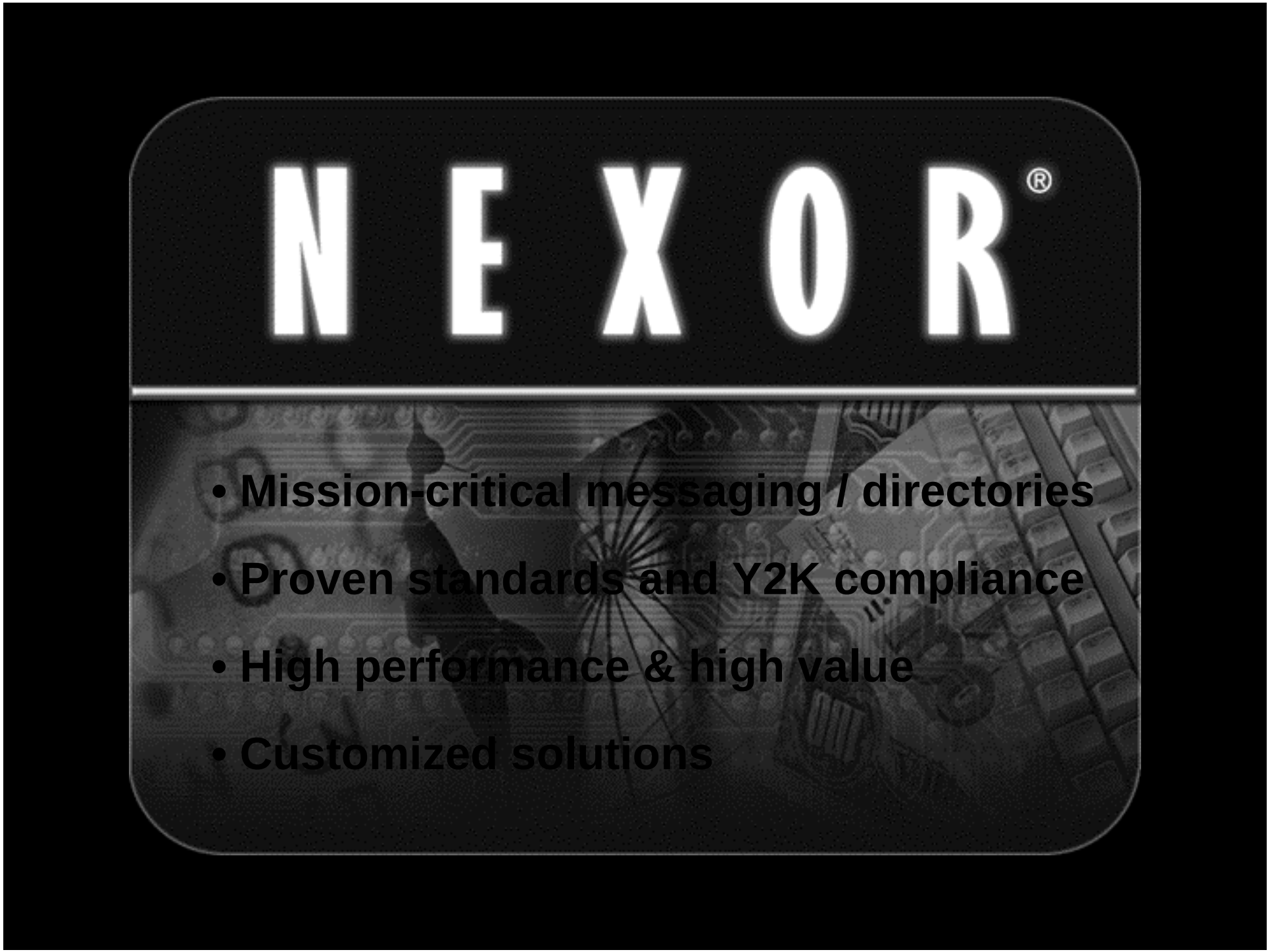
How to contact us

NEXOR, Inc.

18310 Montgomery Village Ave., Suite 100
Gaithersburg, MD 20879
Phone: (301) 258-7000
Fax: (301) 258-7004
Web: www.nexor.com
Internet: info@nexor.com

Bob Johnson

Business Development Manager
Internet: Bob.Johnson@nexor.com
Phone: (301) 258-7000 x230


NEXOR®
• Mission-critical messaging / directories
• Proven standards and Y2K compliance
• High performance & high value
• Customized solutions